

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/003253

International filing date: 22 February 2005 (22.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-053294
Filing date: 27 February 2004 (27.02.2004)

Date of receipt at the International Bureau: 07 April 2005 (07.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

22.02.2005

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2004年 2月27日
Date of Application:

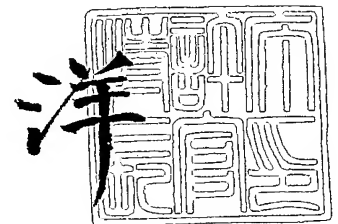
出願番号 特願2004-053294
Application Number:
[ST. 10/C]: [JP2004-053294]

出願人 キヤノン株式会社
Applicant(s):

2005年 3月25日

特許庁長官
Commissioner,
Japan Patent Office

小川



【書類名】 特許願
【整理番号】 260413
【提出日】 平成16年 2月27日
【あて先】 特許庁長官殿
【国際特許分類】 B41J 29/38
【発明者】
 【住所又は居所】 東京都大田区下丸子 3 丁目 3 0 番 2 号 キヤノン株式会社内
 【氏名】 浜田 昇
【特許出願人】
 【識別番号】 000001007
 【氏名又は名称】 キヤノン株式会社
【代理人】
 【識別番号】 100090273
 【弁理士】
 【氏名又は名称】 國分 孝悦
 【電話番号】 03-3590-8901
【手数料の表示】
 【予納台帳番号】 035493
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9705348

【書類名】 特許請求の範囲**【請求項 1】**

ユーザが入力する個人識別コードを受領するコード受領手段と、
乱数を発生させる乱数発生手段と、
前記個人識別コード又はそれに基づく鍵を暗号鍵として前記発生させた乱数を暗号化する乱数暗号化手段と、
前記受領した個人識別コードを所定の関数で変換するコード変換手段と、
前記乱数を暗号鍵として印刷データを暗号化する印刷データ暗号化手段と
を有することを特徴とする情報処理装置。

【請求項 2】

前記コード変換手段は、前記個人識別コードを一方向関数で変換することを特徴とする請求項 1 記載の情報処理装置。

【請求項 3】

前記コード変換手段は、前記個人識別コードのハッシュ値をとる手段であることを特徴とする請求項 2 記載の情報処理装置。

【請求項 4】

さらに、前記暗号化された乱数、前記変換された個人識別コード、前記暗号化された印刷データを送信する送信手段を有することを特徴とする請求項 1 乃至 3 のいずれか 1 項に記載の情報処理装置。

【請求項 5】

暗号化された乱数、所定関数で変換された第 1 の個人識別コード、暗号化された印刷データを受信する受信手段と、
ユーザが入力する第 2 の個人識別コードを受領するコード受領手段と、
前記受領した第 2 の個人識別コードを所定の関数で変換するコード変換手段と、
前記変換された第 1 の個人識別コードと前記変換された第 2 の個人識別コードとが同じ
か否かを判断する判断手段と、
前記変換された第 1 及び第 2 の個人識別コードが同じときには、前記第 2 の個人識別コード又はそれに基づく鍵を暗号鍵として前記暗号化された乱数を復号する乱数復号手段と

、
前記変換された第 1 及び第 2 の個人識別コードが同じときには、前記復号された乱数を暗号鍵として前記暗号化された印刷データを復号する印刷データ復号手段と
を有することを特徴とする印刷制御装置。

【請求項 6】

前記コード変換手段は、前記第 2 の個人識別コードを一方向関数で変換することを特徴とする請求項 5 記載の印刷制御装置。

【請求項 7】

前記コード変換手段は、前記第 2 の個人識別コードのハッシュ値をとる手段であることを特徴とする請求項 6 記載の印刷制御装置。

【請求項 8】

さらに、前記復号された印刷データを印刷処理する印刷処理手段を有することを特徴とする請求項 5 乃至 7 のいずれか 1 項に記載の印刷制御装置。

【請求項 9】

情報処理装置及び印刷制御装置を含む印刷制御システムであって、
前記情報処理装置は、
ユーザが入力する第 1 の個人識別コードを受領するコード受領手段と、
乱数を発生させる乱数発生手段と、
前記第 1 の個人識別コード又はそれに基づく鍵を暗号鍵として前記発生させた乱数を暗号化する乱数暗号化手段と、
前記受領した第 1 の個人識別コードを所定の関数で変換するコード変換手段と、
前記乱数を暗号鍵として印刷データを暗号化する印刷データ暗号化手段と、

前記暗号化された乱数、前記変換された第1の個人識別コード、前記暗号化された印刷データを前記印刷制御装置へ送信する送信手段とを有し、

前記印刷制御装置は、

前記暗号化された乱数、前記変換された第1の個人識別コード、前記暗号化された印刷データを前記情報処理装置から受信する受信手段と、

ユーザが入力する第2の個人識別コードを受領するコード受領手段と、

前記受領した第2の個人識別コードを所定の関数で変換するコード変換手段と、

前記変換された第1の個人識別コードと前記変換された第2の個人識別コードとが同じか否かを判断する判断手段と、

前記変換された第1及び第2の個人識別コードが同じときには、前記第2の個人識別コード又はそれに基づく鍵を暗号鍵として前記暗号化された乱数を復号する乱数復号手段と

、前記変換された第1及び第2の個人識別コードが同じときには、前記復号された乱数を暗号鍵として前記暗号化された印刷データを復号する印刷データ復号手段とを有することを特徴とする印刷制御システム。

【請求項10】

前記情報処理装置及び前記印刷制御装置の前記コード変換手段は、個人識別コードを一方向関数で変換することを特徴とする請求項9記載の印刷制御システム。

【請求項11】

前記情報処理装置及び前記印刷制御装置の前記コード変換手段は、個人識別コードのハッシュ値をとる手段であることを特徴とする請求項10記載の印刷制御システム。

【請求項12】

前記印刷制御装置は、さらに、前記復号された印刷データを印刷処理する印刷処理手段を有することを特徴とする請求項9乃至11のいずれか1項に記載の印刷制御システム。

【請求項13】

ユーザが入力する個人識別コードを受領するコード受領ステップと、

乱数を発生させる乱数発生ステップと、

前記個人識別コード又はそれに基づく鍵を暗号鍵として前記発生させた乱数を暗号化する乱数暗号化ステップと、

前記受領した個人識別コードを所定の関数で変換するコード変換ステップと、

前記乱数を暗号鍵として印刷データを暗号化する印刷データ暗号化ステップとを有することを特徴とする情報処理方法。

【請求項14】

前記コード変換ステップは、前記個人識別コードを一方向関数で変換することを特徴とする請求項13記載の情報処理方法。

【請求項15】

前記コード変換ステップは、前記個人識別コードのハッシュ値をとるステップであることを特徴とする請求項14記載の情報処理方法。

【請求項16】

さらに、前記暗号化された乱数、前記変換された個人識別コード、前記暗号化された印刷データを送信する送信ステップを有することを特徴とする請求項13乃至15のいずれか1項に記載の情報処理方法。

【請求項17】

暗号化された乱数、所定関数で変換された第1の個人識別コード、暗号化された印刷データを受信する受信ステップと、

ユーザが入力する第2の個人識別コードを受領するコード受領ステップと、

前記受領した第2の個人識別コードを所定の関数で変換するコード変換ステップと、

前記変換された第1の個人識別コードと前記変換された第2の個人識別コードとが同じか否かを判断する判断ステップと、

前記変換された第1及び第2の個人識別コードが同じときには、前記第2の個人識別コ

ード又はそれに基づく鍵を暗号鍵として前記暗号化された乱数を復号する乱数復号ステップと、

前記変換された第1及び第2の個人識別コードが同じときには、前記復号された乱数を暗号鍵として前記暗号化された印刷データを復号する印刷データ復号ステップとを有することを特徴とする印刷制御方法。

【請求項18】

前記コード変換ステップは、前記第2の個人識別コードを一方向関数で変換することを特徴とする請求項17記載の印刷制御方法。

【請求項19】

前記コード変換ステップは、前記第2の個人識別コードのハッシュ値をとるステップであることを特徴とする請求項18記載の印刷制御方法。

【請求項20】

さらに、前記復号された印刷データを印刷処理する印刷処理ステップを有することを特徴とする請求項17乃至19のいずれか1項に記載の印刷制御方法。

【請求項21】

請求項13乃至16のいずれか1項に記載の情報処理方法の各ステップをコンピュータに実行させるためのプログラム。

【請求項22】

請求項17乃至20のいずれか1項に記載の印刷制御方法の各ステップをコンピュータに実行させるためのプログラム。

【書類名】明細書

【発明の名称】情報処理装置、印刷制御装置及び印刷制御システム

【技術分野】

【0001】

本発明は、例えばパーソナルコンピュータなどの印刷クライアントから、例えばプリンタなどの印刷デバイスにネットワークを介して印刷ジョブを送信する際に、その印刷ジョブデータを途中の盗聴や改ざんから守るために暗号化して送る暗号化印刷技術に関するものである。

【背景技術】

【0002】

クライアントからネットワークを介して印刷データをプリンタに送って印刷する系においては、経路上で印刷データが盗聴されるあるいは改ざんされるという潜在的な脅威が存在する。

【0003】

また、プリンタにおいて、従来のように自動的に印刷が開始されて排紙されてしまうのであれば、印刷出力を攻撃者が持ち去ってしまうかもしれないという脅威も存在する。

【0004】

これらの脅威に対抗するために、ジョブを暗号化して送り、プリンタでは暗号化したまま保持しておき、ユーザがプリンタまで歩いて行ってジョブを確認した後に、そこで始めて復号および印刷を開始するようにシステムを改良する必要がある。

【0005】

ところが、もしプリンタに複数のジョブが印刷待ちで保持されている場合には、それらのジョブの中から、自分のジョブだけを正しく識別する必要があるが、ジョブ自体が暗号化されているため、全ジョブをスキャンして、ジョブのヘッダ部分に自分のユーザIDに相当するものがあるものだけを抜き出すという従来どおりの方法が使えない。

【0006】

図6は、この問題を概念的に示した模式図である。ホストパーソナルコンピュータ（PC）101および105と印刷機能を持つデバイス102は、ネットワーク104を介して相互に接続されている。今、ホストPC101および105からデバイス102に対して、全部で三つの暗号化印刷ジョブが送られたとする。デバイス102では、これらのジョブを印刷することなしに、暗号化した状態のままデバイス102内部のジョブ保留領域103に保留しておく。

【0007】

ここで、ホストPC101を使っていたあるユーザAがデバイスの前まで歩いて行って、そこで自分の暗号化印刷ジョブの保留を解いて、印刷を開始させようとするものと仮定する。

【0008】

ここで問題になるのは、三つのジョブのうちから、どれがユーザAのジョブかを認識する方法である。

【0009】

ジョブは暗号化されているから、ジョブのヘッダに埋め込まれているはずのユーザ識別子が一致するものを抜き出すという方法は使えない。ユーザ識別子の部分だけを暗号化しないという方法もあるが、それではユーザAが印刷を行ったということ自体の秘密が守れず、セキュリティ上好ましくない。

【0010】

このように、複数のジョブがプリンタに保持されている場合には、正しいジョブを印刷するために、ユーザのジョブを識別するための何らかの方法が必要である。

【0011】

プリンタで保留状態になっているジョブの識別に関しては、例えば次のような方法が開示されている（例えば特許文献1参照）。

【0012】

図7は、特許文献1に示された方法を簡単に説明するための概念図である。特許文献1の方法によれば、ホストPC201がデバイス202に対して印刷データ211を送信する。すると、デバイス202では、その印刷データを一意に識別する暗証コード212を生成し、それをホストPC201に送信する。ホストPC201側でその暗証コード212を受け取ったユーザは、デバイス202の前まで移動して、その暗証コード212をデバイス202に入力することによって、自分のジョブを識別して出力結果を得るというものである。

【0013】

【特許文献1】特開2001-105690号公報

【発明の開示】

【発明が解決しようとする課題】

【0014】

しかしながら、前記特許文献1の方法では、途中、デバイス側からホスト側へ、暗号化印刷ジョブを守るための番号を通知するという安全でない手順を踏む必要がある。

【0015】

さらに、特許文献1では、盗聴を防ぐためのジョブの暗号化については触れられておらず、仮に印刷ジョブが暗号化されていたとしても、攻撃者は印刷データの破壊や、あるいはデバイス側で無意味な印刷結果を出力させることによって紙の無駄遣いをさせる事などを目的として、印刷ジョブの改ざんを試みるかもしれない。このような攻撃に対する備えも必要であるが、前記特許文献1では触れられていない。

【0016】

本発明の目的は、これらの点を改善し、印刷デバイスからホストへジョブを識別するためのID番号を通知するという安全でない手順を踏む必要を無くし、かつ印刷のセキュリティを保つことである。

【課題を解決するための手段】

【0017】

本発明の情報処理装置は、ユーザが入力する個人識別コードを受領するコード受領手段と、乱数を発生させる乱数発生手段と、前記個人識別コード又はそれに基づく鍵を暗号鍵として前記発生させた乱数を暗号化する乱数暗号化手段と、前記受領した個人識別コードを所定の関数で変換するコード変換手段と、前記乱数を暗号鍵として印刷データを暗号化する印刷データ暗号化手段とを有することを特徴とする。

また、本発明の印刷制御装置は、暗号化された乱数、所定関数で変換された第1の個人識別コード、暗号化された印刷データを受信する受信手段と、ユーザが入力する第2の個人識別コードを受領するコード受領手段と、前記受領した第2の個人識別コードを所定の関数で変換するコード変換手段と、前記変換された第1の個人識別コードと前記変換された第2の個人識別コードとが同じか否かを判断する判断手段と、前記変換された第1及び第2の個人識別コードが同じときには、前記第2の個人識別コード又はそれに基づく鍵を暗号鍵として前記暗号化された乱数を復号する乱数復号手段と、前記変換された第1及び第2の個人識別コードが同じときには、前記復号された乱数を暗号鍵として前記暗号化された印刷データを復号する印刷データ復号手段とを有することを特徴とする。

また、本発明の印刷制御システムは、情報処理装置及び印刷制御装置を含む印刷制御システムであって、前記情報処理装置は、ユーザが入力する第1の個人識別コードを受領するコード受領手段と、乱数を発生させる乱数発生手段と、前記第1の個人識別コード又はそれに基づく鍵を暗号鍵として前記発生させた乱数を暗号化する乱数暗号化手段と、前記受領した第1の個人識別コードを所定の関数で変換するコード変換手段と、前記乱数を暗号鍵として印刷データを暗号化する印刷データ暗号化手段と、前記暗号化された乱数、前記変換された第1の個人識別コード、前記暗号化された印刷データを前記印刷制御装置へ送信する送信手段とを有し、前記印刷制御装置は、前記暗号化された乱数、前記変換された第1の個人識別コード、前記暗号化された印刷データを前記情報処理装置から受信する

受信手段と、ユーザが入力する第2の個人識別コードを受領するコード受領手段と、前記受領した第2の個人識別コードを所定の関数で変換するコード変換手段と、前記変換された第1の個人識別コードと前記変換された第2の個人識別コードとが同じか否かを判断する判断手段と、前記変換された第1及び第2の個人識別コードが同じときには、前記第2の個人識別コード又はそれに基づく鍵を暗号鍵として前記暗号化された乱数を復号する乱数復号手段と、前記変換された第1及び第2の個人識別コードが同じときには、前記復号された乱数を暗号鍵として前記暗号化された印刷データを復号する印刷データ復号手段とを有することを特徴とする。

また、本発明の情報処理方法は、ユーザが入力する個人識別コードを受領するコード受領ステップと、乱数を発生させる乱数発生ステップと、前記個人識別コード又はそれに基づく鍵を暗号鍵として前記発生させた乱数を暗号化する乱数暗号化ステップと、前記受領した個人識別コードを所定の関数で変換するコード変換ステップと、前記乱数を暗号鍵として印刷データを暗号化する印刷データ暗号化ステップとを有することを特徴とする。

また、本発明の印刷制御方法は、暗号化された乱数、所定関数で変換された第1の個人識別コード、暗号化された印刷データを受信する受信ステップと、ユーザが入力する第2の個人識別コードを受領するコード受領ステップと、前記受領した第2の個人識別コードを所定の関数で変換するコード変換ステップと、前記変換された第1の個人識別コードと前記変換された第2の個人識別コードとが同じか否かを判断する判断ステップと、前記変換された第1及び第2の個人識別コードが同じときには、前記第2の個人識別コード又はそれに基づく鍵を暗号鍵として前記暗号化された乱数を復号する乱数復号ステップと、前記変換された第1及び第2の個人識別コードが同じときには、前記復号された乱数を暗号鍵として前記暗号化された印刷データを復号する印刷データ復号ステップとを有することを特徴とする。

また、本発明のプログラムは、上記の情報処理方法の各ステップをコンピュータに実行させるためのプログラムである。

また、本発明のプログラムは、上記の印刷制御方法の各ステップをコンピュータに実行させるためのプログラムである。

【発明の効果】

【0018】

印刷制御装置（例えば印刷デバイス）から情報処理装置（例えばホスト）へ印刷データを守るための番号を通知するという安全でない手順を踏むこと無しに、印刷データを暗号化して送ることができ、かつ印刷制御装置側において印刷データの識別も可能になる。また、印刷データを途中で改ざんされる危険を回避することができる。

【発明を実施するための最良の形態】

【0019】

（第1の実施形態）

図2は、一般的なコンピュータの内部構成を示したものであり、本発明の第1の実施形態のホストPC101あるいは印刷デバイス102のコントローラも同様の構成を取るものである。

【0020】

図2において、300はコンピュータ全体である。コンピュータ300は、ROM302あるいは例えばハードディスクなどの大規模記憶装置311に記憶されたソフトウェア（コンピュータプログラム）を実行するCPU301を備え、システムバス304に接続される各デバイスを総括的に制御する。312は、タイマーである。

【0021】

303はRAMで、CPU301の主メモリ、ワークエリア等として機能する。305は外部入力コントローラ（KBD C）で、コンピュータに備えられた各種ボタンあるいはキーボード309等からの指示入力を制御する。306はディスプレイコントローラ（DISPC）で、表示モジュール（DISPLAY）310の表示を制御する。

【0022】

記憶装置コントローラ 307 は、ハードディスクなどの大規模記憶装置 311 に対するアクセスを制御する。

【0023】

308 はネットワークインタフェースカード (NIC) で、LAN104 を介して、他のネットワーク機器あるいはファイルサーバ等と双方向にデータをやりとりする。

【0024】

図 6 に、本実施形態の暗号化印刷システムの構成例を示す。ホスト PC101 および 105 と印刷機能を持つ印刷デバイス (プリンタ) 102 は、ネットワーク 104 を介して相互に接続されている。例えば、ホスト PC101 及び/又は 105 がデバイス 102 に対して、3 つの暗号化印刷ジョブを送信したとする。デバイス 102 では、これらのジョブを印刷することなしに、暗号化した状態のままデバイス 102 内部のジョブ保留領域 103 に保留しておく。その後、ユーザがデバイス 102 に対して所定の操作を行うことにより、暗号化されたジョブが復号されて印刷される。

【0025】

図 1 は、本実施形態における印刷ジョブデータの暗号化方法とジョブの識別方法を示す図である。

【0026】

ホスト PC101 では、印刷ジョブを暗号化するために、乱数 rnd を発生させ、それを PDL (ページ記述言語: Page-Description Language) データの暗号鍵として用いる。乱数 rnd は、ユーザが入力した PIN (個人識別番号: Personal Identification Number) コードをハッシュした値 k によって暗号化される。値 k もハッシュされ、後にデバイス 102 側において暗号化ジョブの識別のために用いられる。なお、PIN は番号以外に文字列を用いたものでもよい。

【0027】

暗号化された PDL データを C とし、PDL データの暗号鍵のハッシュ値 k を B とし、乱数 rnd を値 k で暗号化したものを A とし、A、B および C の三つの組をデバイス 102 側に送信する。

【0028】

A、B および C を受信したデバイス 102 では、ユーザが入力した PIN のハッシュ値を計算し、これを k' とする。次に k' のハッシュ値を計算し、これを B' とする。受信したデータの一部である B と B' が同一かどうかによって、前記 PIN を入力したユーザのジョブかどうかを判断し、前記ユーザのジョブである場合にはデータを復号して印刷する。

【0029】

図 3 は、図 1 におけるホスト PC101 側におけるジョブの暗号化手順を示したフローチャートである。

【0030】

図 3 の手順は、ホスト PC101 上の CPU301 によって実行される。さらに前提として、印刷すべき文書や画像等のデータは、プリンタドライバモジュールによってプリンタが読解可能な形式、すなわち PDL データに変換され、それが図 4 の手順を実施するモジュールに順次受け渡されるものとする。

【0031】

印刷データの送出にあたっては、まずステップ 501 において、外部入力コントローラ 305 を制御して、ユーザが入力装置 309 を用いて打ち込む PIN コードを受領する。続くステップ 502 において、乱数 rnd を発生させる。なお、この rnd は、後のステップにおいて、PDL データを暗号化するために用いられる。続くステップ 503 において、前記ステップ 501 で受領した PIN コードを基に、ジョブを暗号化するための暗号鍵をさらに暗号化するための暗号鍵 k を計算する。本実施形態においては、PIN コードを例えば MD5 や SHA-1 などのハッシュ関数に入力し、出力のハッシュ値を暗号鍵 k として用いるものとする。続くステップ 504 において、前記ステップ 503 で計算した

値 k を暗号鍵として、PDL データを暗号化するための鍵 rnd を暗号化し、これを A とする。なお、PIN コードを暗号鍵としてもよい。続くステップ 505 において、前記ステップ 503 で計算した値 k のハッシュ値を計算し、これを B とする。続くステップ 506 において、前記ステップ 502 で発生させた乱数 rnd を暗号鍵として、印刷のための PDL データを暗号化し、これを C とする。続くステップ 507 において、前記ステップ 504 で計算した A と前記ステップ 505 で計算した B と前記ステップ 506 で計算した C を、RAM 303 上の一時記憶領域に用意したバッファに格納して送信に備えてひとまとまりにする。続くステップ 508 において、NIC 308 を制御して、前記ステップ 507 で用意した送信データを LAN 104 を介してデバイス 102 に送信する。送信が完了したら、RAM 303 上のバッファを解放する。

【0032】

図 4 は、図 1 におけるデバイス 102 側における、ジョブの識別方法と復号手順を示したフローチャートである。デバイス 102 は、ホスト PC 101 が送信した上記の送信データを受信する。

【0033】

図 4 の手順は、デバイス 102 上の CPU 301 によって実行される。

デバイスでのジョブの識別と復号にあたっては、まずステップ 601 で、入力コントローラ 305 を制御して、ユーザが入力部 309 を介して入力する PIN コードを受領する。続くステップ 602 で、前記ステップ 601 で受領した PIN コードのハッシュ値 k' を計算する。続くステップ 603 で、前記ステップ 602 で計算した k' のハッシュ値を計算し、これを B' とする。続くステップ 604 において、デバイス 102 内部のジョブ保留領域 103 (図 6) に保留されている全ジョブがジョブ識別処理を行われたかどうかを判断する。

【0034】

もし全ジョブが処理完了されたと判断されたら、本手順を終了する。

もし全ジョブが処理完了されていないと判断されたら、ステップ 605 に進む。ステップ 605 では、処理対象ジョブのヘッダ部分から値 B を取り出し、前記ステップ 603 で計算した値 B' と同じかどうかを判断する。

【0035】

もし同じであると判断されたら、ステップ 606 に進み、ジョブのヘッダ部分から値 A を取り出して、それを前記ステップ 602 で計算した値 k' を暗号鍵として、復号処理を行う。そして得られた値を rnd' とする。

【0036】

続くステップ 607 において、ジョブから暗号化された PDL データ C を取り出し、それを前記ステップ 606 で計算した値 rnd' を暗号鍵として、復号処理を行う。そして得られた値が、印刷すべき PDL データである。続くステップ 608 では、前記ステップ 607 で得た PDL データを印刷処理する。

【0037】

ステップ 608 の処理が終了したら、あるいはステップ 605 において B と B' が同じではないと判断された場合には、ステップ 604 に戻り、次のジョブに対して処理を続行する。

【0038】

上記で説明した本実施形態に係るホスト PC 101 あるいはデバイス 102 のプログラムは、外部からインストールされるプログラムによって、ホスト PC 101 あるいはデバイス 102 によって実行されても良い。その場合、そのプログラムは CD-ROM やフラッシュメモリ やフレキシブルディスクなどの記憶媒体により、あるいは電子メール やパソコン通信などのネットワークを介して、外部の記憶媒体からプログラムを含む情報群をホスト PC 101 あるいはデバイス 102 上にロードすることにより、ホスト PC 101 あるいはデバイス 102 に供給される場合でも本発明は適用されるものである。

【0039】

図5は、記憶媒体の一例であるCD-ROMのメモリマップを示す図である。9999はディレクトリ情報を記憶してある領域で、以降のインストールプログラムを記憶してある領域9998および印刷クライアントあるいはネットワークプリンタの制御プログラムを記憶してある領域9997の位置を示している。9998は、インストールプログラムを記憶してある領域である。9997は、印刷クライアントあるいはネットワークプリンタの制御プログラムを記憶してある領域である。本実施形態の印刷クライアントあるいはネットワークプリンタの制御プログラムがホストPC101あるいはデバイス102にインストールされる際には、まずインストールプログラムを記憶してある領域9998に記憶されているインストールプログラムがシステムにロードされ、CPU301によって実行される。次に、CPU301によって実行されるインストールプログラムが、デバイス制御プログラムを記憶してある領域9997から印刷クライアントあるいはネットワークプリンタの制御プログラムを読み出して、ROM302の内容を書き換えるか、あるいは大規模記憶装置311にインストールする。この場合、ROM302は単純なマスクROMではなく、フラッシュROMなどの書き換え可能なROMである必要がある。

【0040】

なお、本実施形態は、複数の機器（例えばホストコンピュータ、インタフェース機器、リーダなど）から構成されるシステムあるいは統合装置に適用しても、ひとつの機器からなる装置に適用してもよい。

【0041】

また、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはCPUやMPU）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、本発明の目的が達成されることは言うまでもない。

【0042】

この場合、記憶媒体から読み出されたプログラムコード自体が本発明の新規な機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【0043】

プログラムコードを供給するための記憶媒体としては、例えば、フレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、CD-R、磁気テープ、不揮発性のメモリカード、ROMなどを用いることができる。

【0044】

また、コンピュータが読み出したプログラムコードを実行することによって、前述した実施形態の機能が実現される他、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているOSなどが実際の処理の一部または全部を行い、その処理によっても前述した実施形態の機能が実現され得る。

【0045】

さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行い、その処理によっても前述した実施形態の機能が実現され得る。

【0046】

なお、本発明は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体から、そのプログラムをパソコン通信など通信ラインを介して要求者にそのプログラムを配信する場合にも適用できることは言うまでもない。

【0047】

（第2の実施形態）

本発明の第2の実施形態を説明する。第1の実施形態では、PDLデータを暗号化するための暗号鍵rndを、さらに暗号化するための鍵として、ユーザが入力したPINコー

ドをハッシュした値を用いたが、特にこの方法に限るものではなく、PINコードを基にした一方向性関数で、変換された後の値の一致性が確認できるものであれば何でも良い。

【0048】

例えば、ハッシュを計算する回数を一回ではなく、出力結果をさらにハッシュ関数に入力して二回ハッシュをかける方法でも良いし、ある決まった数とPINコードとのXORを取って、そのハッシュ値を得ることを複数回繰り返すということでも良い。

【0049】

当然、これらの場合には、デバイス側でジョブを識別するにあたって、PINを扱う方法を、ホストPC側で用いた方法と同様の方法にする必要がある。

【0050】

以上のように、第1及び第2の実施形態では、ホスト側において、ユーザが入力するPINコードを受け取る手段と、乱数を発生させる手段と、前記発生させた乱数を暗号化する手段と、前記受け取ったPINコードを容易に推測することができない値に変換する手段と、印刷ジョブデータを暗号化する手段とをもたせる。

【0051】

さらに、デバイス側において、ユーザが入力するPINコードを受け取る手段と、受信した暗号化ジョブの真正性を確認する手段と、暗号化ジョブの暗号鍵を計算する手段と、暗号化ジョブを復号する手段とを持たせる。

【0052】

デバイスからホスト側へ印刷ジョブを守るための番号を通知するという安全でない手順を踏むこと無しに、印刷データを暗号化して送ることができ、かつデバイス側においてジョブの識別も可能になる。また、印刷データを途中で改ざんされる危険も回避することができる。すなわち、ジョブを識別するためのIDを乱数値で自動生成し、かつその乱数値を暗号化するなど、改ざん検知を含めてセキュリティを保つことができる。

【0053】

なお、上記実施形態は、何れも本発明を実施するにあたっての具体化の例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその技術思想、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。

【図面の簡単な説明】

【0054】

【図1】実施形態の暗号化印刷方法の仕組みを示す図である。

【図2】実施形態のホストPCあるいは印刷デバイスの内部構成を示す図である。

【図3】実施形態におけるホストPCの動作を示すフローチャートである。

【図4】実施形態における印刷デバイスの動作を示すフローチャートである。

【図5】実施形態のソフトウェアの記憶媒体におけるメモリマップを示す図である。

【図6】暗号化印刷におけるジョブ識別問題を示す概念図である。

【図7】従来技術におけるジョブ識別方法の一例を示す図である。

【符号の説明】

【0055】

309、501、601 PINコード受領手段

502 乱数発生手段

504 乱数暗号化手段

503、505、602、603 PINコード変換手段

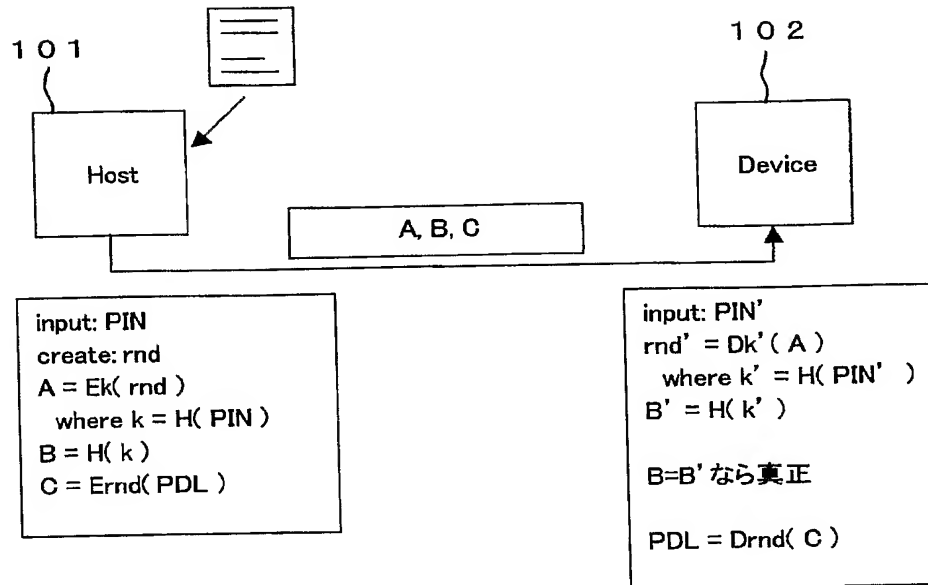
506 印刷データ暗号化手段

605 ジョブ識別手段

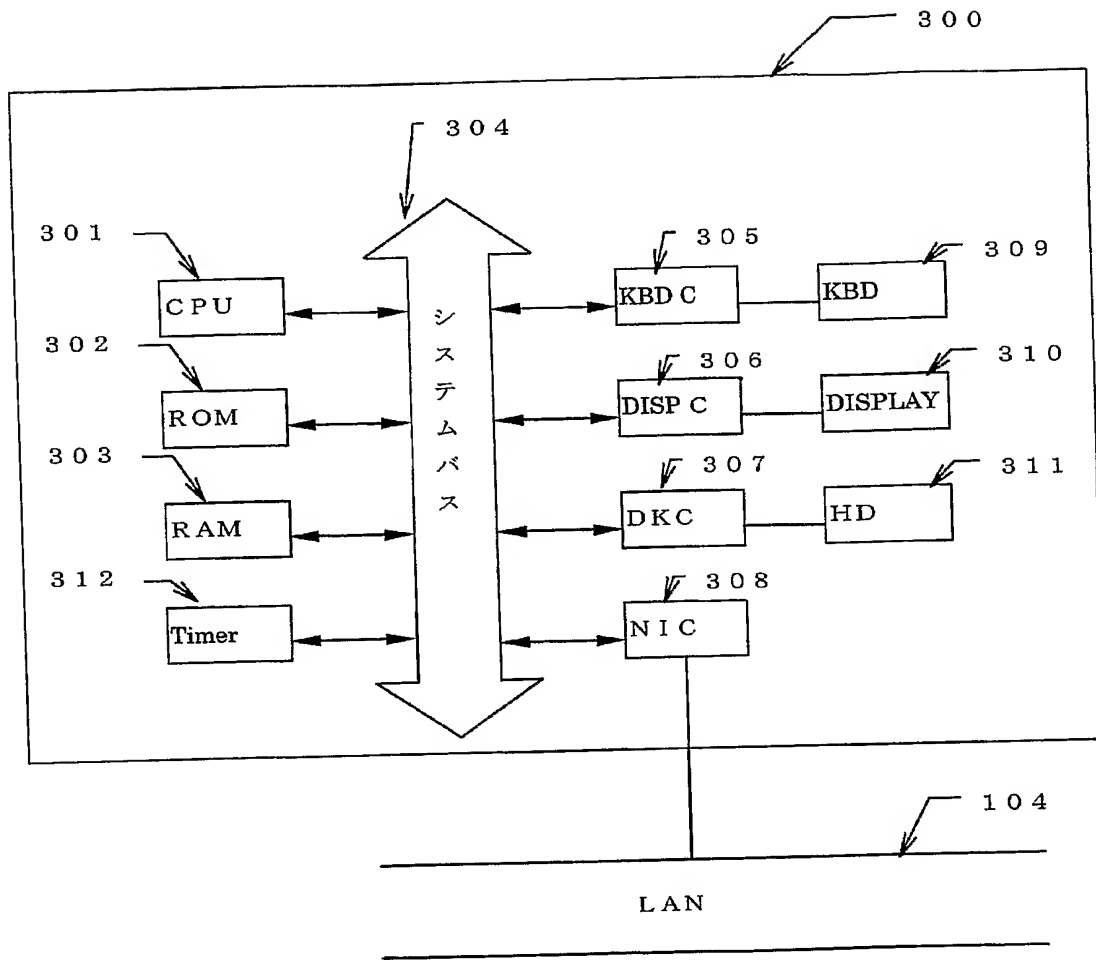
606 暗号鍵計算手段

608 印刷データ復号化手段

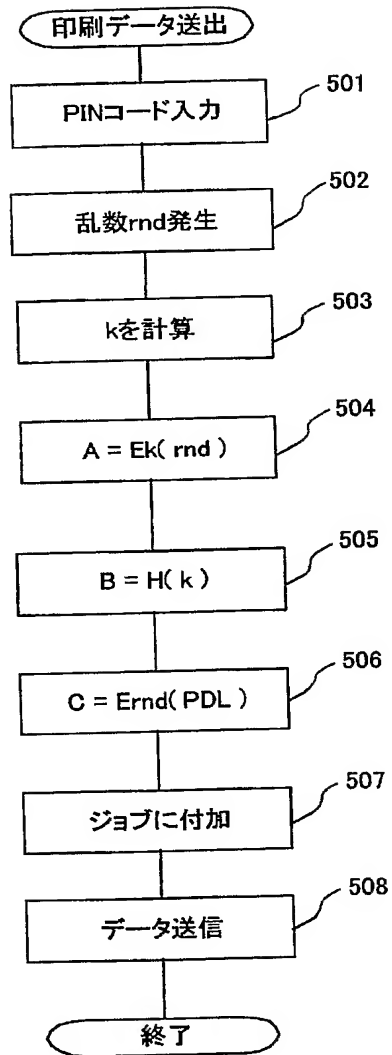
【書類名】 図面
【図 1】



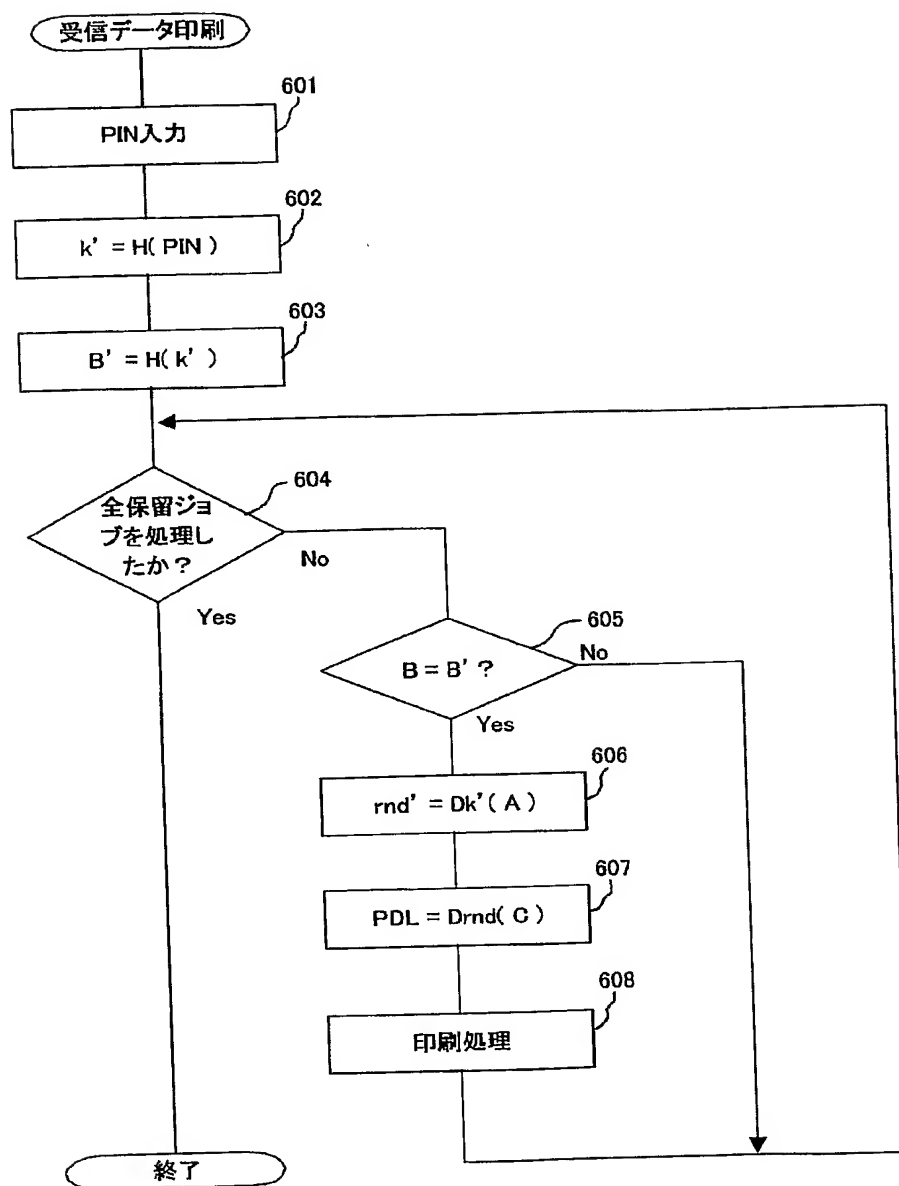
【図 2】



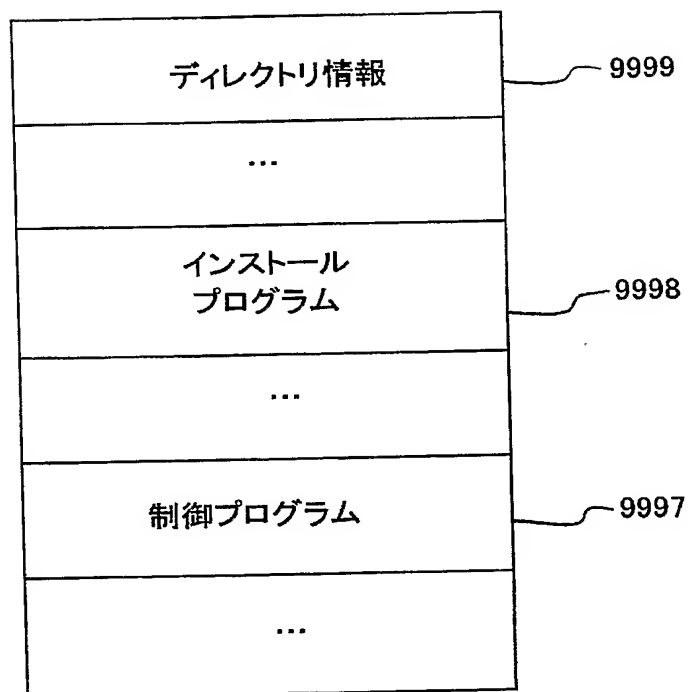
【図 3】



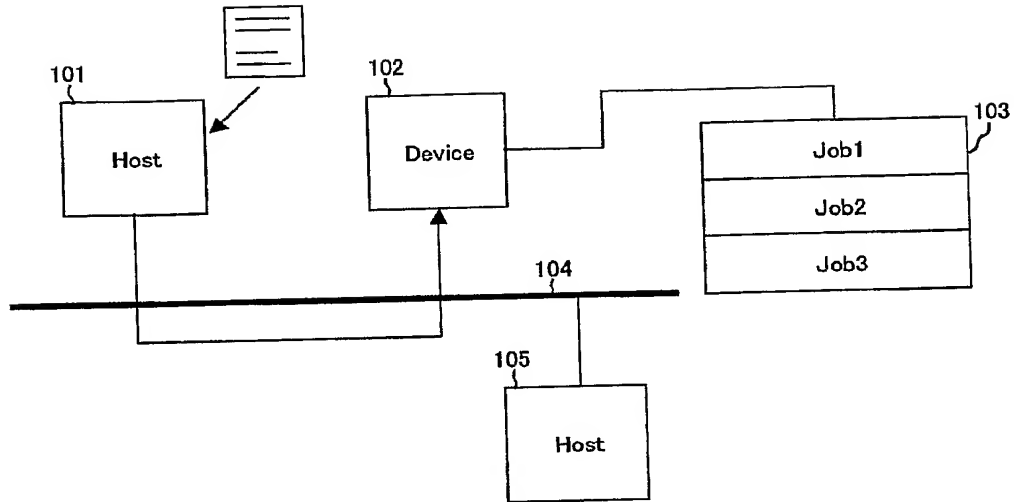
【図 4】



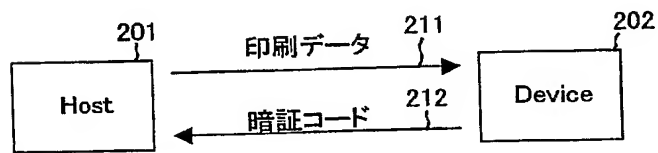
【図 5】



【図 6】



【図 7】



【書類名】 要約書

【要約】

【課題】 印刷デバイスからホストへジョブを識別するためのID番号を通知するという安全でない手順を踏む必要を無くし、かつ印刷のセキュリティを保つことを課題とする。

【解決手段】 ユーザが入力する個人識別コード(PIN)を受領するコード受領手段と、乱数(rnd)を発生させる乱数発生手段と、個人識別コード又はそれに基づく鍵を暗号鍵として発生させた乱数を暗号化する乱数暗号化手段と、受領した個人識別コードを所定の関数で変換するコード変換手段と、乱数を暗号鍵として印刷データ(PDL)を暗号化する印刷データ暗号化手段とを有する情報処理装置が提供される。

【選択図】 図1

特願 2 0 0 4 - 0 5 3 2 9 4

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 1 0 0 7]

1. 変更年月日

[変更理由]

住 所

氏 名

1 9 9 0 年 8 月 3 0 日

新規登録

東京都大田区下丸子 3 丁目 3 0 番 2 号

キャノン株式会社